

Open Source Election
Technology Institute Inc.
530 Lytton Avenue, 2nd Floor
Palo Alto, California 94301 USA
+1.650.600.1450
hello@osetinstitute.org



Monday, 15 May 2023

Harry F. Martin

**Courtroom Deputy Clerk
to the Hon. Amy Totenberg**
2388 United States Courthouse
75 Ted Turner Dr., S.W.
Atlanta, Georgia 30303-3309
404.215.1437

via eMail: Harry_Martin@gand.uscourts.gov

May it Please the Court —

My name is Gregory A. Miller, and I have been authorized by our Board of Directors to submit this amicus curiae letter on behalf of the OSET Institute, Inc.—a 501(c)(3) non-profit non-partisan election technology research organization involving over 70 election and technology professionals headquartered in Palo Alto, CA., with over 17-years of experience at the intersection of election technology design and cybersecurity.

This letter regards a question in the matter of Donna Curling et al v. Brad Raffensperger et al, Civil Action No. 1:17-CV-2989-AT in the United States District Court for the Northern District of Georgia, Atlanta Division; the Honorable Judge Amy Totenberg presiding.

The Court asks the following question:

Plaintiffs have argued that the posting of the Dominion software on the Internet by third party actors poses an aggravated threat of hacking and harm to election security and Plaintiffs' voting rights, in tandem with other occurrences within Coffee County's election operations. In light of this, how is it that publication of the redacted version of Dr. Halderman's report, which contains a virtual roadmap of how the Dominion software and system may be compromised, would not compound the threats and risks to the security of the computerized voting system that Plaintiffs' counsel focus on as a central theme of their legal claims, evidence, and argument? Or is this combined threat irrelevant and, if so, for what reasons?

On behalf of the OSET Institute's senior technical team including the Chief Technology Officer, we provide our view for the Court's consideration hereunder.



On careful review of the matter through ours lens of critical infrastructure cybersecurity technology, best practices, and public policy, we conclude that the report on security flaws in Dominion voting machines, authored by Professors J. Alex Halderman and Drew Springall in July 2021 (“Halderman Report”) and placed under seal by the Federal District Court for the Northern District of Georgia, should be immediately unsealed by the Court and be made public.

No one at the OSET Institute, including myself, has seen or read Professor Halderman’s report, since it remains under seal. However, from what we have learned of it from other professional colleagues in academia and elsewhere, it appears the report is a solid example of a standard security-vulnerability report, now ready for public release. Our understanding is that the report has been available for over 500 days at this point, and under best cybersecurity practices we submit that such is more than enough time to have repaired the reported vulnerabilities that can be satisfactorily and successfully remediated. It is our further understanding, pursuant to a recent U.S. EAC compliance filing, that the manufacturer, Dominion, has claimed to have repaired at least some of the vulnerabilities in their Democracy Suite 5.17 product that can apparently be traced to the Halderman Report findings.

Accordingly, best practices indicate it is time to disclose this report. Customers of this Dominion product, which primarily includes election administrators, public officials, and voters, require complete information about the security of the technology in order to reach their own properly informed conclusions about how to proceed with this equipment in their own elections. Publication of the report will allow that analysis to occur, and as a consequence will likely ensure that all remediations are, in fact, made. Moreover, there is no benefit to the integrity of the existing Dominion technology in sustaining the nondisclosure of the Halderman Report. It is uniformly understood by computer security professionals including CISA, that keeping digital vulnerabilities secret does not sustain or improve security. If someone can discover a vulnerability, others can do the same.

Let us return our attention to the very specific question the Court asks regarding the potential for disclosure to aggravate pre-existing disclosures and their potential to cause harm to the integrity of affected elections equipment.

The existing voting systems in use in Georgia are critical information systems that are now vulnerable to attack by skilled adversaries who already have complete information about these



target critical infrastructure systems, via prior unauthorized examination of the software code and data which was previously made available, and quite probably via Internet publication. Access to the content of the redacted Halderman report would not provide these adversaries with any additional attack capability beyond the capabilities that they now have, given prior full access to the technology via those prior disclosures.

We agree that the Halderman Report could be characterized by analogy as a “virtual roadmap” of the target systems’ vulnerabilities. Extending this analogy, we observe that adversaries already have a far better map—in essence a complete satellite and topographic map, which is the knowledge already gained by direct access to the unauthorized disclosures of the technology and related data earlier. Accordingly, the publication of the Halderman Report will not increase the attackers’ already complete navigational knowledge and capability of the technology.

This brings us to the Court’s second question:

“Or is this combined threat irrelevant and, if so, for what reasons?”

We observe that we published a position statement on the dangers of unauthorized disclosures of critical infrastructure technology last July.¹ We stand by that statement and do not see our encouragement of immediate publication of the Halderman Report as being at odds with that position. First, we submit that the open threat we discuss in our July 2022 statement, plus the fixed and known set of issues in the Halderman Report do not combine to form a “combined threat.” They are two separate situations; one is a set of known threats that should have been addressed by now, 500 days after the report, and the other, is a remaining open-ended situation of ongoing potential for new attacks including at least misinformation and at worst, potential for subversive compromise.

Further, we would not characterize the threats as entirely irrelevant. One cannot guarantee that every customer of the product has taken the recommended steps to remove the vulnerabilities. However, the standard and best practice is, once responsible disclosure has occurred, and there has been time for remediation, to be public about the existence of the vulnerability and the fact that there are fixes. That’s sound policy, otherwise every vendor would hide information about every vulnerability, and lack the incentive to increase quality and security of

¹ See: <https://www.osetinstitute.org/research/2022/1407/votingsys-disclosures>



their product. That's one reason why it is good policy, and there's no reason not to apply it to Dominion. We either accept the residual risk of some customers who have not responded to the vulnerability, and gain the benefit of standard disclosure policies; or we must have zero tolerance for any residual risk, and accept the consequences of vendors being able to hide any and every vulnerability with impunity, unless or until it is business-wise economically feasible for their remedy.

Finally, we note that the prior unauthorized disclosures of the technology have already provided a head start for any adversary, and the Halderman Report will serve little to no incremental value to their efforts or plans for misdeeds.

Therefore, for the foregoing reasons, we respectfully encourage the immediate release of the Halderman Report for its public benefit, as no additional harm can come from so-doing; however, not allowing its publication creates a different harm as a matter of public policy and best cybersecurity practices.

Respectfully Submitted,

A handwritten signature in blue ink, appearing to read "Gregory A. Miller", written over a circular blue stamp or seal.

Gregory A. Miller

Co-Founder & Chief Operating Officer

gam@osetinstitute.org | +1 503.703.5150